Stephen Cobb, CISSP
Senior Vice President
Research & Education

May 20, 2002

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

.This statement is submitted on behalf of ePrivacy Group, a privacy consulting, training and technology company, as part of our contribution to the Federal Trade Commission's public workshop on Consumer Information Security, held on May 20-21, 2002. As a company dedicated to solving data privacy problems for both companies and consumers, ePrivacy Group applauds the FTC's efforts in organizing and hosting the workshop. We share many of FTC's concerns regarding the security of consumer information, whether it is being stored on the consumer's computer, held in company databases, or traveling somewhere in between. ePrivacy Group appreciates this opportunity to participate as a panelist in the workshop to discuss the business of protecting consumer information. The following statement provides further information and background on some of the points raised by the panel.

Panel III: What Business Models Help Consumers Maintain Security?

Business models that help consumers secure their information are vitally important to three overlapping constituencies: consumers; the companies with whom they do business; and the country as a whole. Unless workable consumer information security business models can be developed and sustained, a significant percentage of consumers will continue to feel, understandably, that their privacy is at risk in our increasingly connected and highly data-dependent society.

The consequences for companies, and the economy, could be chilling. Surveys have repeatedly shown that the fears of consumers concerning the safety of their personal information act as a brake upon the growth of electronic commerce. Security breaches and privacy incidents continue to rattle consumer confidence in the "new economy." A significant percentage of consumers now worry, and not without reason, about everything from file-corrupting virus infections to privacy-invading hackers, from the annoyance of intrusive email and telemarketers to the expense of fraudulent credit card charges, from the trauma of lost data to the nightmare of full-blown identity theft.

There will also be serious consequences for our country if the millions of powerful computers used by consumers, many of whom now access the Internet via high-speed broadband connections, continue to be vulnerable to penetration and subversion. As Richard Clarke, Special Advisor to the President for Cybersecurity, has repeatedly stressed, securing America' critical infrastructure will not be possible as long as the computing resources its citizens can be used against it.

ePrivacy Group

Paoli Executive Green III
Suite 300
43 Leopard Road
Paoli, PA 19301
tel 1.610.407.0400
fax 1.610.407.7085

www.eprivacygroup.com

As the personal computer evolved from specialized business tool to ubiquitous consumer information appliance, several business models and strategies emerged with respect to security. The four most basic models can be defined: integrated; bundled; add-on; and service.

Integrated: Consumers can buy a security capability that is integrated into a product, such as file encryption that is part of an application, such as a spreadsheet, or even part of the operating system.

Bundled: Consumers can acquire a security capability that is bundled with another product, such as an anti-virus program that comes with their new computer.

Add-on: Consumers can purchase a security capability separately, such as a firewall acquired to sit between a home computer and a broadband Internet connection.

Service: Consumers can obtain security as a service, typically under a subscription pricing model, such as firewall protection or email-virus scanning provided by an Internet Service Provider (ISP).

An Example of Business Models: Computer Virus Protection

These basic models, and several other elements of security business models, are readily apparent if we look, by way of example, at the evolution of computer virus protection. The first mass market anti-virus products, which emerged in the 1980s, were add-ons, something you bought if you were concerned enough about the virus problem to spend money on protection. In 1993, one year after the Michelangelo virus scare, a major operating system vendor decided to integrate anti-virus (AV) capability into the operating system (OS). The result was Microsoft MS-DOS Version 6. This particular offering was somewhat short-lived and numerous AV vendors continued to sell their products direct to consumers, either as add-ons or bundled with other products.

In the mid-nineties, the efforts of AV vendors were hampered by a combination of misleading product claims from unscrupulous vendors and the inherent difficulty of verifying product claims for anti-virus products. This led to the emergence of an industry-funded, independent anti-virus testing service, provided by the National Computer Security Association ("NCSA" which later became ISCA Labs). Consumers who bought NCSA-approved AV software could rest assured that the product met reasonable and clearly stated standards. The effects on the industry, and the results for consumers, were enormously positive. Through a combination of criticism and cooperation the NCSA standard was constantly improved by input from other NGOs such as EICAR, Virus Bulletin, and the Wild List.

While independent testing brought respectability to the AV industry, the overall effectiveness of the products themselves continued to be hampered by the failure of customers to actually use the product or use it appropriately. Numerous studies, including extensive surveys conducted annually by NCSA, indicated that the root causes of this behavior were twofold: ignorance and annoyance. Customers did not know enough about the inner workings of computer viruses and AV software, resulting in behavior which defeated the latter and paved the way for the former. Furthermore, customers found the

inconveniences imposed by AV regimens to be annoying, resulting in lapses which enabled virus infections to continue to occur. The response of the AV industry was twofold: education of customers and improvement of products.

Unfortunately, some AV companies found that the cost of educating the consumer market was just too high. Despite several industry-wide efforts at AV education, such as an annual virus scan day, too much of the consumer education was happening post-purchase; that is, via AV company help lines (which are notoriously costly to fund). Product development, in the direction of totally transparent, fully-automated virus prevention also proved expensive. This led some vendors to exit the consumer market in favor of developing enterprise-oriented products.

Other vendors found new pricing models and new approaches to integration and bundling. For example, AV software has, at times, been integrated with other applications that range from backup and maintenance products to communication products. And for several years now, leading PC vendors have bundled one or more AV products leading AV companies, pre-installed on computers sold to consumers. However, bundled AV protection is not always turned on by default. Furthermore, the product will not remain effective beyond an initial trial period unless updated, which typically requires additional payment from the consumer. This is because the most widely used anti-virus protection technology, scanning for known signatures, requires frequent updates to recognize new threats.

For these reasons, some AV companies have adopted a service model to finance the cost of creating and distributing those updates. The service model, which requires periodic subscription payments to maintain the security capability, can either work on its own, selling the service as a security add-on to consumers who have no AV software, or in combination with a free bundling of the initial installation (based on the vendor's assumption that an acceptable percentage of users who start out with their bundled AV product will be converted to subscription users of their product).

Elements of Consumer Information Security Business Models

The preceding example illustrates the main elements of security business models. We will briefly recap them before describing some of the ways in which these elements can be combined to provide a viable approach to the business of consumer information security.

1. Integrated: providing security capabilities as part of the operating system or an application.

2. Bundled: including a security product with other products.

3. Add-on: the retailing of security products that consumers can purchase if they wish to acquire such capabilities.

4. Subscription: providing ongoing security services in return for a periodic payment which funds the updating of the security capability.

5. Independent Third Party: an entity which brings objectivity and standards to the marketplace (may include underwriting the product claims which vendors make to

consumers, voicing consumer concerns to vendors, dispute resolution for customers, qualifying companies for regulatory safe harbor through certification to, or compliance with, third party standards).

6. Best Practices: industry associations encouraging best practices among member companies in order increase confidence in the industry and its products.

7. Market Education: educating consumers so that they can make informed decisions when purchasing and using products, as well as setting realistic expectations and encouraging responsible behavior.

8. Self-regulation: actions taken by companies to uphold standards, adhere to best practices, and support the efforts of independent third parties (such actions can reduce the need for government regulation, or create a model for less burdensome implementation of regulations when there are present).

9. Regulation: by government agencies enforcing legislation or applying legal principles such as fair business practices (although the AV industry itself is not regulated, some laws can be construed to require the use of its products).

The element of regulation merits further discussion in the context of this FTC workshop. While there is no industry-specific regulation of the computer security industry, agencies of the government, such as the FTC and State Attorneys General, have provided a framework of fair trade practices within which the industry has evolved. Furthermore, all three branches of the government have encouraged, in various ways, the deployment and refinement of computer security capabilities. These efforts includes security technology research by various agencies, numerous national infrastructure protection initiatives, and the promulgation of security standards in support of legislated privacy protections in sectors such as healthcare and financial services (e.g. the Safeguards Rule for personal financial information, recently finalized by the FTC).

The Privacy Perspective

Society's growing concern over the privacy of personal information has helped turn the spotlight on consumer information security. Rules and regulations and standards are being put in place to govern the handling of personally identifiable information within many companies. Agencies such as the FTC have shown that they will hold all companies to the promises they make to consumers regarding privacy. Yet the protection of personal information at the consumer end, for example, when stored on the family computer, remains problematic (a problem we identified in 1996, during research on privacy protection for patient information, as "the leaky client").

Obviously, consumers have a responsibility to protect their own information; but it is just as obvious that today's consumers are under-equipped for this task. This is not to say there are no tools or sources of assistance available. Several companies represented at the Workshop supply security tools. Several of the comments submitted to the Workshop describe steps that are being taken to assist consumers. These include educational initiatives, such as Stay Safe Online, privacy and trust seals such as TRUSTe and BBB Online, and security standards, established either by industry groups such as American Community

Bankers and VISA, or by government agencies, such HHS and the FTC. What is missing is the right combination of means, motive, and financial opportunity to move consumer information security to the next level. Clearly, finding the right business models to do this will be an important part of that movement.

A Sample Business Model

By way of illustration, we would like to briefly describe a business model we have developed to enhance privacy and data protection in a specific area, email. We will not take time here to describe the threats that email poses to privacy and security but refer to the FTC's web site which offers a lot of useful information on this topic. We do note that that consumers use the Internet for email more than for anything else, and we think anyone who uses email today will agree that it is in serious need of improvement.

At ePrivacy Group we began developing a set of technologies called Postiva to do just that, starting with a seal that can be placed in email to verify the identity of senders and their adherence to responsible, privacy-sensitive email practices. But even as we began development we could see that our technology alone would not be enough to solve the problem. After all, technologies like encryption, integrity checking, and virus scanning have been around for a long time but are still grossly under-deployed. We needed a broader business model and set about building one from the elements outlined above. The following paragraphs describe how our model was built.

Best Practices: We turned to industry associations to learn about, and then work to improve, best practices in the area of commercial email. There are many forms of email that consumers want to receive from companies, ranging from discounts on airline tickets to online purchase and shipping confirmations and account management correspondence. Today, this email arrives in the consumer's in-basket alongside, and often difficult to distinguish from, a large and growing volume of email that is unwanted, known in the vernacular as spam (a significant percentage of spam is associated with fraud, pornography, and other objectionable material, some of which poses a direct threat to the security of consumer information). Much of the legitimate, permission-based email marketing done is this country originates from companies belonging to the Direct Marketing Association ("DMA") and its subsidiary, the Association for Interactive Marketing ("AIM"). By working with these organizations we were able to develop a set of privacy-sensitive email marketing principles to which responsible companies could agree. This provided our technology, which enforces compliance with these principles, a solid basis for widespread acceptance and support.

Independent Third Party: Our technology can place a stamp in outbound email that gives the recipient assurances about the message and its sender. To make sure consumers have a high level of confidence in those assurances we wanted independent third-party oversight. TRUSTe offered an established track record of trust assurance, consumer education, dispute resolution, and regulatory safe harbor. So we established an alliance with TRUSTe to deliver what is now called the Trusted Sender program.

Market Education: We know that our technology will not succeed unless we educate consumers about the need for, and appropriate use of, privacy protection products. So we have launched several initiatives, via our web site, speaking engagements, articles, industry

associations, and our relationship with TRUSTe, which has a number of educational programs. We have also committed resources to the International Association of Privacy Officers (IAPO) to foster professional development in corporate privacy management.

Self-Regulation: Through our work with industry associations and trusted third parties we are contributing to the kind of self-regulation which benefits both vendors and consumers. Our technology itself enables some of the improvements to email that lawmakers are seeking to achieve through legislation. It certainly allows companies to demonstrate adherence to privacy-sensitive best practices with respect to email which may mitigate the need for additional regulation. Agencies such as the FTC have shown willingness to provide "safe harbor" to companies who participate in self-regulation programs and agree to private third party dispute resolution.

Regulation: Security companies certainly need to be aware of legislation that could either regulate their products or even accelerate their adoption. As developers of technology to improve email, we monitor legislation that might regulate email. Not surprisingly, we try to make lawmakers aware of the Trusted Sender program's ability to enable self-regulation. We have not lobbied for or against any specific legislation but have provided several briefings to lawmakers and regulators to help them better understand the technical issues involved in such legislation and the potential for unintended consequences.

Integrated/ Bundled/Add-on: Widespread adoption of our email technology will not happen unless it is integral to applications that consumers use. We designed the first phase of the program to work automatically with standard email clients. No plug-ins or downloads are required. For the next phase, we are working with vendors of email clients to make added functionality an integral part of the installed product.

Subscription: At the right price point, funding ongoing data privacy services through periodic payments can be an attractive model for both vendors and consumers. However, we still see consumer resistance to additional fees for greater security or privacy. Greater market education may change this, but we think we have found a funding model for commercial email that imposes no new costs on consumers. Instead we leverage the need that responsible companies have to distinguish their email from spam. For consumer this means fewer problems with unwanted email and greater protection and control of personal information. Companies get the ability to better target their messages, to the consumers who want, and are even pleased, to receive them.

Summary

Viable business models for consumer information security are possible. They may require creative new alliances; the money to pay for them may need to be sought somewhere outside the traditional buyer-seller relationship; they may need the encouragement and support of government agencies; but they are possible. Our own business model is still evolving, along with our company, but we hope that this presentation of the key elements of such models, and our examples of some of the ways in which they can be applied, will help other companies succeed in their efforts to deliver consumer information security to the market in a sustainable way. Clearly, successful business models for consumer security offer great benefits to consumers, to companies, and to our country. We thank the FTC for organizing this Workshop and providing this opportunity to participate.